

Amendments to the Specification

Please make the following amendments to the specification.

Please insert the following paragraph on page 1 after the title:

--RELATED APPLICATION

This is a Continuation of International Application PCT/JP02/00743, filed January 31, 2002, which is hereby incorporated by reference in its entirety.--

Please replace paragraphs starting at page 4 line 21 to page 6, line13 with the following amended paragraphs:

That is, a random number generator as set forth herein ~~in claim 4~~ is characterized by comprising a flip-flop in which an output state (0 or 1) becomes definite according to a phase difference between signals inputted to two input units, a delay unit for producing the phase difference between these two input signals, and a feedback circuit for controlling the phase difference of the delay unit so that an occurrence ratio of 0 or 1 of an output from the flip-flop by the input signals is constant within a specified repetition cycle.

Besides, a random number generator as set forth herein ~~in claim 2~~ is characterized in that the delay unit comprises a delay circuit for delaying the input signals at several stages and outputting them, and a selection circuit for selecting one of delay outputs according to a select input.

Besides, a random number generator as set forth herein ~~in claim 3~~ is characterized in that the feedback circuit comprises a first counter for measuring the specified repetition cycle of the input signals, a second counter for measuring the number of occurrences of 0 or 1 of the output from the flip-flop in every repetition cycle, a register for holding a measurement output of the second counter every repetition cycle, a constant setter for generating comparison data for setting of the occurrence

ratio of 0 or 1 of the output from the flip-flop, a comparator for comparing output data of the register with the comparison data, and a reversible counter for generating a select signal of the selection circuit on the basis of a comparison output of the comparator.

In the structure of the invention ~~claim 1 to claim 3~~, the natural random number generator, which relates to the generation of a random number, has uniformity, and has no regularity, no correlativity and no periodicity, can be realized entirely by the digital circuits. Besides, by suitably setting the repetition cycle of the input signals and the resolution of the set phase difference in the delay unit, a lot of random numbers can be generated at high speed. Further, because of the digital circuit structure, it is easy to cope with the formation as an LSI.

Besides, a random number generator as set forth herein ~~in claim 4~~ is characterized in that a random number outputted from the flip-flop, or a random number constructed by scrambling the former random number is used as set data of the repetition cycle set for the first counter and the comparison data of the comparator.

Please replace the paragraphs starting at page 6, line 16 to page 7, line 16 with the following amended paragraphs:

Besides, a random number generator as set forth herein ~~in claim 5~~ is characterized by comprising an auxiliary random number generating unit having a same structure as the random number generator as set forth herein ~~in claim 3~~, in which a random number from the auxiliary random number generating unit is used as set data of the repetition cycle set for the first counter and the comparison data of the comparator.

Besides, a random number generator as set forth herein ~~in claim 6~~ is characterized by comprising an auxiliary random number generating unit having a same structure as the random number generator as set forth herein ~~in claim 3~~, in which a random number from the auxiliary random number generating unit and a random number constructed by scrambling a random number from the random number generator are used as set data of the repetition cycle set for the first counter and the comparison data of the comparator.

In the structure of above claim 5 and claim 6, since the random number data from the auxiliary random number generating unit is not entirely outputted to the outside (outside of the random number generator), it is impossible to predict the property, tendency, periodicity and the like of the generated random number, and a complete natural random number can be formed.

Besides, a random number generator as set forth herein in claim 7 is characterized in that a waveform shaping circuit is added to an input signal line of the flip-flop.

Please replace the paragraph at page 7, lines 21-24 with the following amended paragraph:

Besides, a random number generator as set forth herein in claim 8 is characterized by comprising an initial control circuit for setting the comparison data of the comparator to 0 for a specified period when power is turned on.

Please replace the paragraphs at page 8, line 2 to line 15 with the following amended paragraphs:

Besides, a random number generator as set forth herein in claim 9 is characterized in that a D-type flip-flop or an R-S flip-flop is used as the flip-flop.

Besides, a random number generator as set forth herein in claim 10 is characterized by comprising a plurality of the random number generators as set forth above in claim 1 arranged in parallel to one another. A mutual relation does not exist entirely between the respective random number generators constituting this parallel type random number generator. Besides, each of the random number generators has no regularity, no correlativity and no periodicity.

Besides, a probability generator as set forth herein in claim 11 is characterized by comprising the random number generator ~~as set forth in claim 1~~.

Please replace the paragraphs at page 9, line 18 to page 10, line 20 with the following amended paragraphs:

That is, a random number generator as set forth herein ~~in claim 12~~ in which a phase difference between two input signals inputted to a flip-flop is automatically adjusted to make an occurrence ratio of 1 or 0 of an output from the flip-flop constant, wherein a jitter generation circuit including a source for generating a noise, an amplifier circuit for amplifying the noise, and a mixer circuit for generating jitter in the input signals by the amplified noise signal is added to an input line of the flip-flop.

Besides, a random number generator as set forth herein ~~in claim 13~~ is constructed by adding the jitter generation circuit to both input lines of the flip-flop.

Besides, a random number generator as set forth herein ~~in claim 14~~ is constructed by adding the jitter generation circuit to any one of input lines of the flip-flop, and adding an integration circuit for delay time correction to the other of the input lines.

Here, in the structure as set forth above ~~in claims 12 to 14~~, the jitter is generated in the input signals inputted to the flip-flop, and the indefinite operation range of the flip-flop is extended. By this, it becomes possible to easily generate a more complete natural random number with uniformity and without regularity, correlativity and periodicity.

Besides, a random number generator ~~according to claim 15~~ is constructed by adding latch means for latching an output of the jitter generation circuit every repetition cycle of the input signals.

Please replace the paragraph at page 10, line 24 to page 11, line 5 with the following amended paragraph:

Besides, a random number generator as set forth herein ~~in claim 16~~ in which a phase difference between two input signals is automatically adjusted to make an occurrence ratio of 1 or 0 of an output from a flip-flop constant, wherein a phase-voltage conversion circuit for converting the phase difference between the two input signals into a voltage is added to a data input line of the flip-flop.

Please replace the paragraphs at page 11, lines 14-17 with the following amended paragraph:

Besides, in a random number generator as set forth herein ~~in claim 17~~, the phase-voltage conversion circuit is constructed by adding enable means operating only at an operation permissible time.

Please replace the paragraph at page 11, line 22 to page 12, line 2 with the following amended paragraph:

Besides, a random number generator as set forth herein ~~in claim 18~~ is constructed by adding a jitter generation circuit including a source for generating a noise, an amplifier circuit for amplifying the noise, and a mixer circuit for generating jitter in the input signals by the amplified noise signal to an output of the phase-voltage conversion circuit.

Please replace the following paragraph at page 12, lines 8-11 with the following amended paragraph:

Besides, in a random number generator as set forth herein ~~in claim 19~~, the jitter generation circuit is constructed by adding enable means operating only at an operation permissible time.

Please replace the following paragraph at page 12, line 16 to page 17, line 16 with the following amended paragraphs:

Besides, in a random number generator as set forth herein ~~in claim 20~~, the mixer circuit includes an integration circuit, and a series connection circuit of a series P-channel transistor circuit and a series N-channel transistor circuit respectively having, as inputs, the integration output signal and the amplified noise signal.

Besides, in a random number generator as set forth herein ~~in claim 21~~, the mixer circuit is also constructed by a series transistor circuit of an N-channel transistor and a P-channel transistor having, as an input, a combined signal of the amplified noise signal and the input signal.

Besides, a random number generator as set forth herein ~~in claim 22~~ in which a phase difference between two input signals inputted to an R-S flip-flop is automatically adjusted to make an occurrence ratio of 1 or 0 of an output from the flip-flop constant, wherein a P-channel transistor is connected in series to a power supply side of an R side gate circuit or an S side gate circuit of an internal transistor circuit constituting the R-S flip-flop, an N-channel transistor is connected in series to a GND side, a source for generating a noise and an amplifier circuit for amplifying the noise are connected to inputs of the P-channel transistor and the N-channel transistor, and a threshold voltage of one of the gate circuits is changed by the amplified noise signal.

Besides, a random number generator as set forth herein ~~in claim 23~~ in which a phase difference between two input signals inputted to an R-S flip-flop is automatically adjusted to make an occurrence ratio of 1 or 0 of an output from the flip-flop constant, wherein a P-channel transistor is connected in series to a power supply side of an R side gate circuit and an S side gate circuit of an internal transistor circuit constituting the R-S flip-flop, an N-channel transistor is connected in series to a GND side, a source for generating a noise and an amplifier circuit for amplifying the noise are connected to inputs of the P-channel transistor and the N-channel transistor, and threshold voltages of both of the gate circuits are changed by the amplified noise signal.

In the R-S flip-flop, when a phase difference between the rising of the R side input signal and the rising of the S side input signal is made to approach 0, a metastable phenomenon occurs. When this phenomenon occurs, it takes a time until the output of the flip-flop becomes definite, and an output state after a given time becomes 0 or 1, or holding of the threshold voltage, or an oscillation state. Here, in the structure as set forth above ~~in claim 22 and claim 23~~, by changing the threshold voltage of the R side and/or S side gate circuit, the metastable state can be instantaneously made the stable state of 1 or 0. Then, the phase difference between the two input signals is automatically adjusted so that the occurrence ratio of 1 or 0 of the output from the flip-flop becomes constant.

Besides, in a random number generator as set forth herein ~~in claim 24~~, the amplifier circuit includes a series input circuit of a capacitor and a resistor, and a series

circuit of a P-channel transistor and an N-channel transistor, and a resistor intervenes between an input and an output of the transistor circuit.

Besides, in a random number generator as set forth herein ~~in claim 25~~, the amplifier circuit includes a series input circuit of a capacitor and a resistor, and a series circuit of a P-channel transistor and an N-channel transistor, and a resistor and a capacitor intervenes in parallel between an input and an output of the transistor circuit.

Besides, in a random number generator as set forth herein ~~in claim 26~~, the amplifier circuit is made to have a multi-stage structure.

Here, in the structure above ~~of claim 24 to claim 26~~, when frequency characteristics of a Low Pass Filter and a High Pass Filter are suitably set according to an after-mentioned noise generation source, the amplifier with suitable characteristics can be realized. Besides, when a MOS transistor is used for the construction, the influence of temperature and power supply fluctuation can be lessened, and a stable operation can be obtained.

Besides, in a random number generator as set forth herein ~~in claim 27~~, the source for generating the noise is constructed by connecting a P-channel transistor and an N-channel transistor in series and short-circuiting an input and an output.

Besides, in a random number generator as set forth herein ~~in claim 28~~, the source for generating the noise is also constructed by connecting a P-channel transistor and an N-channel transistor in series and making a resistor intervene between an input and an output.

Besides, in a random number generator as set forth herein ~~in claim 29~~, the source for generating the noise is constructed by connecting a P-channel transistor and an N-channel transistor in series, making a resistor intervene between an input and an output, and making a series circuit of a resistor and a capacitor intervene between the input and GND.

Besides, in a random number generator as set forth herein ~~in claim 30~~, the source for generating the noise is constructed by connecting a P-channel transistor and an N-channel transistor in series, making a resistor intervene between an input and an

output, and making a series circuit of a resistor and a capacitor intervene between the input and a power supply.

Besides, in a random number generator as set forth herein ~~in claim 31~~, the source for generating the noise is constructed by short-circuiting an input and an output of an N-channel transistor, and making a resistor intervene between the output and a power supply.

Besides, in a random number generator as set forth herein ~~in claim 32~~, the source for generating the noise is constructed by making a resistor intervene between an input and an output of an N-channel transistor, and by making a resistor intervene between the output and a power supply.

Besides, in a random number generator as set forth herein ~~in claim 33~~, the source for generating the noise is constructed by short-circuiting an input and an output of a P-channel transistor, and by making a resistor intervene between the output and GND.

Besides, in a random number generator as set forth herein ~~in claim 34~~, the source for generating the noise is constructed by making a resistor intervene between an input and an output of a P-channel transistor, and by making a resistor intervene between the output and GND.

Here, in the structure as set forth herein ~~in claim 27 to claim 34~~, since a faint thermal noise generated from the circuit element (transistor, resistor, capacitor, or combination of these) in the active state is used as the source for generating the noise, it can be realized by a simple circuit structure and very inexpensively.

Besides, a probability generator as set forth herein ~~in claim 35~~ is constructed by using the random number generator ~~as set forth in claim 12~~.

Please replace the paragraphs at page 18, line 20 to page 20, line 13 with the following amended paragraphs:

That is, the invention as set forth herein ~~in claim 36~~ is a random number generator comprising a flip-flop in which an output state (0 or 1) becomes definite according to a phase difference between two input signals, a phase adjustment unit for

adjusting phases of the input signals, and a feedback circuit unit for controlling the phase difference so that an occurrence ratio of 0 or 1 of an output from the flip-flop by the input signals converges on a given value within a specified repetition cycle, wherein the phase adjustment unit includes coarse adjustment means of a phase and fine adjustment means operating in sequence.

Besides, according to the invention as set forth herein ~~in claim 37~~, in the random number generator as set forth herein ~~in claim 36~~, each of the coarse adjustment means and the fine adjustment means includes a delay circuit for delaying the input signals at several stages and outputting them, a selection circuit for selecting one of delay outputs according to a select input, and a reversible counter for controlling the select input according to the phase difference.

In the structure as set forth above ~~in claim 36 or claim 37~~, the coarse adjustment and fine adjustment of the phase are performed, so that it becomes possible to enlarge a phase adjustment range and to make an efficient phase adjustment.

Besides, the invention as set forth herein ~~in claim 38~~ is a random number generator comprising a flip-flop in which an output state (0 or 1) becomes definite according to a phase difference between two input signals, a phase adjustment unit for adjusting phases of the input signals, and a feedback circuit unit for controlling the phase difference so that an occurrence ratio of 0 or 1 of an output from the flip-flop by the input signals converges on a given value within a specified repetition cycle, wherein the phase adjustment unit includes a delay circuit for delaying the input signals at several stages and outputting them, a selection circuit for selecting one of delay outputs according to a select input, and a reversible counter for controlling the select input according to the phase difference, and includes a control circuit for comparing a normal distribution of the occurrence ratio of 0 or 1 with the number of times of occurrence of 0 or 1 within the repetition cycle and making a count number of the reversible counter variable according to a position of the normal distribution to which the number of times of occurrence corresponds.

Please replace the paragraph at page 20, line 21 to page 21, line 1 with the following amended paragraph:

Besides, the invention as set forth herein ~~in claim 39~~ is constructed by comprising, in the random number generator as set forth herein ~~in claim 36~~, an initial control circuit for making the repetition cycle shorter than the repetition cycle at a normal operation time for a given period from power activation.

Please replace paragraphs at page 21, lines 5-18 with the following amended paragraphs:

The invention as set forth herein ~~in claim 40~~ is constructed by adding, in the random number generator as set forth herein ~~in claim 36~~, a noise generation source and a noise/phase converter to both input lines of the flip-flop.

Further, the invention as set forth herein ~~in claim 41~~ is constructed by adding, in the random number generator as set forth herein ~~in claim 36~~, a noise generation source and a noise/phase converter to any one of input lines of the flip-flop.

In the structure above ~~of claim 40 or claim 41~~, jitter is generated in the signals inputted to the flip-flop, and the indefinite operation range of the flip-flop is extended. By this, it becomes possible to generate a natural random number with uniformity and without regularity, correlativity and periodicity at high speed and with high accuracy.

Please replace the paragraphs at page 22, line 11 to page 26, line 13 with the following amended paragraphs:

Besides, among the inventions, the invention above ~~of claim 43~~ comprises, instead of the output circuit, a comparator for comparing previously set upper limit comparison data and lower limit comparison data with the data held in the register to output a verification signal.

Besides, among the inventions, the invention above ~~of claim 44~~ comprises a random number generating unit for outputting "1" and "0" as random number data, a data holding unit for holding previous random number data outputted from this random number generating unit, a comparator for comparing present random number data

outputted from the random number generating unit with the previous random number data held in the data holding unit, outputting a count up signal when both are identical to each other, and outputting a count clear signal when both are different from each other, a counter for counting up when the count up signal is received from the comparator and clearing count when the count clear signal is received from the comparator, and an output circuit for outputting data held in this counter as verification data.

Besides, among the inventions, the invention above ~~of claim 45~~ comprises a random number generating unit for outputting "1" and "0" as random number data, a data holding unit for holding previous random number data outputted from this random number generating unit, a first comparator for comparing present random number data outputted from the random number generating unit with the previous random number data held in the data holding unit, outputting a count up signal when both are identical to each other, and outputting a count clear signal when both are different from each other, a counter for counting up when the count up signal is received from the first comparator and clearing count when the count clear signal is received from the first comparator, a register for holding output data of this counter, a second comparator for comparing the data of this register with the output data of the counter, outputting a data overwrite signal when the latter is larger than the former, and outputting a data hold signal at a time other than that, a control circuit for performing a control to write the output data of the counter into the register when the data overwrite signal is received from the second comparator, and to hold the data of the register when the data hold signal is received from the second comparator, and an output circuit for outputting the data held in the register as verification data.

Besides, among the inventions, the invention above ~~of claim 46~~ comprises, instead of the output circuit, a third comparator for comparing previously set comparison data with the data held in the register to output a verification signal.

Besides, among the inventions, the invention above ~~of claim 47~~ is constructed by comprising a random number generating unit for outputting "1" and "0" as random number data, a first counter for counting a given number of times, a data holding unit for holding previous random number data outputted from the random number generating

unit, a comparator for comparing present random number data outputted from the random number generating unit with the previous random number data held in the data holding unit, outputting a count up signal when both are identical to each other, and outputting a count clear signal when both are different from each other, a second counter for counting up when the count up signal is received from the comparator and clearing count when the count clear signal is received from the comparator, a decoder for decoding output data of the second counter to output it for respective signal lengths, plural third counters for respectively counting output data of the decoder for the respective signal lengths, plural registers for respectively holding output data of the respective third counters every given number of times counted by the first counter, and a control circuit for performing a control to output verification data from the respective registers on the basis of a signal in every given number of times counted by the first counter and output data of the comparator.

Besides, among the inventions, the invention above ~~of claim 48~~ is constructed by providing a selection circuit for selecting and outputting the output data of the registers.

Besides, among the inventions, the invention above ~~of claim 49~~ is constructed by connecting a plurality of the one-bit random number generators in parallel to each other and providing a selection circuit for selecting verification data outputted from these one-bit random number generators for every bit and outputting them.

Besides, among the inventions, the invention above ~~of claim 50~~ is constructed by connecting a plurality of the one-bit random number generators in parallel to each other and providing a selection circuit for selecting verification signals outputted from these one-bit random number generators for every bit and outputting them.

Besides, among the inventions, the invention above ~~of claim 51~~ is constructed by comprising the one-bit random number generator, a shift register for converting the random number data outputted from the one-bit random number generator from serial data to parallel data, a counter for counting a bit length of given parallel data, a register for holding the parallel data of the shift register in every cycle counted by the counter, and a comparator for comparing previously set probability upper limit data and

probability lower limit data with the parallel data held in the register to output a probability signal.

Further, among the inventions, the invention above of ~~claim 52~~ is constructed by comprising the multi-bit random number generator, and a comparator for comparing previously set probability upper limit data and probability lower limit data with random number data outputted from the multi-bit random number generator to output a probability signal.